Notice of Allowability	Application No.	Applicant(s)	
	09/663,664	CHESS ET AL.	
	Examiner	Art Unit	
	Carl Colin	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *7/28/2006 and interview on 11/6/2006*.

2. ☒ The allowed claim(s) is/are *1-22 and 25-44*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413), Paper No./Mail Date *20061106* .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/09/06

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with John S. Sensny on November 6, 2006 and e-mail received on November 9, 2006.

The application has been amended as follows:

Claim 1. (Currently Amended) A method, comprised of enhancing a computational service to each client of a plurality of clients, by:

moving a selected portion of a computation from a server into a trusted co-server executing inside a secure coprocessor;

allowing each client to interact with the server and the co-server; and

using the trusted co-server as a trusted third party to authenticate interactions between the client and the server; and

wherein the moving step includes the steps of

i) installing a device private/public key pair on the co-server,

ii) installing co-server application software in the trusted co-server, said ~~co-sever~~ co-server application software having an ability to authenticate itself using said device key pair,

iii) the co-server application software then generating an application key pair including a public key and a private key, [[;]]

iv) using the co-server application's ability to authenticate itself ~~and~~ with said device key pair to prove to a certificate authority that said application key pair belongs to an installation of said ~~co-sever~~ co-server application,

v) the certificate authority then issuing a certificate attesting to the public key of said application key pair and the entity to which said public key belongs, and

vi) the co-server application storing said certificate,

the step of using the trusted co-server includes the steps of

i) establishing a session between the client and the co-server application, and

ii) indicating to the client that the co-server application demonstrates knowledge of the private key of said application key pair to provide assurance of the authenticity of communication from the trusted co-server.

Claim 3. (Currently Amended) A method as recited in Claim 1, wherein said step of allowing includes enabling said each client an authenticated, private channel to said co-server.

Claim 5. (Currently Amended) A method as in Claim 3, wherein said step of enabling includes the said each client using the co-server's certified application keypair to establish a shared symmetric key.

Claim 8. (Currently Amended) A method as in Claim 1, wherein said ~~step of~~ enhancing includes providing a desired security and/or privacy property.

Claim 9. (Currently Amended) A method as in Claim 1, wherein said ~~step of~~ enhancing includes providing at least one security and/or privacy property to an application selected from the group including: authentication of clients, nonrepudiation of client activity, nonrepudiation of server activity, credit card transaction security, taxes on e-commerce activity, re-selling of intellectual property, privacy of sensitive or proprietary web activity, correctness of web activity, enforcement of logo and/or "seal of approval" licenses, safety of downloadable content, authenticity of downloadable content, integrity of server machine, and any combination of these.

Claim 10. (Currently Amended) A method as in Claim 1, wherein:

input from said client is prompt from server for the user's private ~~authenticator~~ authentication data, input from said server is this authentication data, and a co-server algorithm that generates output to a client based on said current co-server state and said inputs indicates whether or not the ~~authenticator~~ authentication data is correct for this user.

Claim 11. (Currently Amended) A method as in Claim [[1]] 10, where the co-server algorithm that generates output to said ~~server~~ client based on a current co-server state and inputs includes a signed statement, using a private key known to the co-server, attesting, for the server, that the client engaged in an interaction satisfying certain properties.

Claim 12. (Currently Amended) A method as in Claim [[1]] 10, where the co-server algorithm that generates output to said client based on a current co-server state and inputs includes a signed statement, using a privacy key known to the co-server, attesting, for the client, that the server engaged in an interaction satisfying certain properties.

Claim 13. (Currently Amended) A method as in Claim [[1]] 10, wherein:

the ~~client's~~ input from said client includes a credit card number (CCN), the output co-server algorithm that generates output to said client based on a current co-server state and inputs includes the CCN, encrypted so that the server cannot read [[it]] the CCN but an acquirer can.

Claim 14. (Currently Amended) A method as in Claim 13, wherein:

the ~~server's~~ input from said server includes a transaction amount, the output co-server algorithm that generates output to said client based on a current co-server state and inputs includes the transaction amount, cryptographically bound to the encrypted CCN so that the server cannot alter [[it]] the transaction amount.

Claim 15. (Currently Amended) A method as in Claim [[1]] 10, where:

the ~~client's~~ input from said client includes a credit card number (CCN), the ~~server's~~ input from said server includes a transaction amount, the co-server encrypts this CCN so that the server cannot read [[it]] the CCN but an acquirer can, and cryptographically binds the transaction amount to ~~the~~ this encrypted CCN, then, at some point during or after the interaction,

transmits this data to the acquirer in such a manner so that the acquirer can receive this transaction exactly once.

Claim 16. (Currently Amended) A method as in Claim 1, wherein:

the ~~interaction via the server input and/or the client input, includes~~ interactions include a transaction amount A, ~~the~~ co-server input ~~may include~~ includes an accumulated total, ~~the~~ a function co-server algorithm that generates a new co-server state based on a current co-server state and inputs updates the accumulated ~~amount~~ total by adding T(A), where T is a predefined function, and at some point during or after this interaction, the co-server produces an authenticated statement of the current value of the accumulated ~~amount~~ total.

Claim 17. (Currently Amended) A method as in Claim [[1]] 10, where:

a remote party is an owner of intellectual property, the ~~server~~ input from the server includes part of this property, encrypted so that only the co-server can decrypt [[it]] said part, the ~~output function~~ co-server algorithm that generates output to said client based on a current co-server state and inputs ~~to the client includes~~ include a portion of a decryption of input from said client.

Claim 18. (Currently Amended) A method as in Claim [[17]] 10, ~~except~~ where the ~~output function~~ co-server algorithm that generates output to said client based on said current co-server state and said inputs ~~now~~ includes a transformation of a portion of ~~the~~ a decryption of input from said server, where said transformation ~~may include~~ includes adding a watermark.

Claim 19. (Currently Amended) A method as in Claim [[17]] 10, ~~except~~ where the ~~output function now~~ co-server algorithm includes a transformation of a portion of ~~the~~ a decryption of input from said server, where said transformation ~~may include~~ includes reducing the quality of the plaintext.

Claim 20. (Currently Amended) A method as in Claim [[17]] 10, ~~except~~ where the ~~output function now~~ co-server algorithm includes a portion of ~~the~~ a decryption of input from said server, re-encrypted~~, possibly with rights management rules,~~ in a manner that a secure coprocessor at the client site can decrypt [[it]] said server.

Claim 21. (Currently Amended) A method as in Claim 1, wherein:

the establishing step includes the step of the client providing input ~~includes~~ including a choice of which record R in a set of records the client would like to receive, the co-server includes this record R in its response to the client, however, the co-server obtains R in such a way as the server does not know which record was the one selected.

Claim 22. (Currently Amended) A method as in Claim 1, wherein:

a remote party establishes a content evaluation scheme, consisting of an evaluation function mapping content to some set of indicators, and as part of computing the client output ~~function~~ co-server algorithm ~~that generates output to said client based on a current~~

~~co-server state and inputs~~, the co-server calculates, or verifies an external calculation, of the evaluation function and includes the result in the client output.

Claim 25. (Currently Amended) A method as in Claim [[24]] 22, where the evaluation function is parameterized by a "signature file" and where the ~~client~~ output to the client includes an identification of which signature file was used in this interaction.

Claim 26. (Currently Amended) A method as in Claim 22, where ~~party~~ the remote party has injected the evaluation function and/or some of its parameters into the co-server through a private channel, so that the server cannot know the details of the evaluation function execution occurring on the co-server.

Claim 27. (Currently Amended) A method as in Claim 22, where input from the server ~~input~~ includes both content and a signature on the content, ~~from one of possibly many content providers,~~ and the evaluation function includes testing whether the signature is valid.

Claim 28. (Currently Amended) A method as in Claim 1, where:

a remote party establishes a content evaluation scheme, consisting of an evaluation function mapping content to some set of indicators, and as part of computing the server output ~~function~~ co-server algorithm, ~~that generates output to said client based on a current co-server state and inputs or internal function co-server algorithm that generates new co-server state based on said current co-server state and said inputs~~ the co-server calculates, or verifies an

external calculation, of the evaluation function ~~input from said client~~ and includes the result in the output.

Claim 29. (Currently Amended) A method as in Claim 1, where:

the co-server has the ability to carry out security-enhancing actions against the server, and ~~the~~ output returned to the client indicates which of these actions have been carried out, and how recently.

Claim 30. (Currently Amended) A method as in Claim 1, where:

the client can specify whether the interaction is a read interaction or a write interaction;

for a write interaction:

the client input includes a message M and a specification S of the appropriate entities who can read this message;

the co-server retains M and S by storing them in some combination across the co-server and server via an algorithm that generates new co-server state based on said current co-server state and said inputs, the internal state in the co-server and co-server algorithm that generates output to said server based on a current co-server state and inputs;

~~however~~ in said write interaction:

any portion of M sent via co-server algorithm that generates output to said server based on said current co-server state and said inputs is encrypted, so that the server cannot access the plaintext;

and mechanisms are used to ensure that, when the co-server later retrieves any of this data from the server, that the data has not been changed;

for a read interaction:

the client input specifies which message M the client would like to read, the co-server retrieves S; if the client satisfies S, then the co-server sends M back to the client, after first retrieving and decrypting ~~it, if necessary~~ M.

Claim 31. (Currently Amended) A method for enhancing a service to provide security and/or privacy to each client ~~from~~ of a plurality of clients, said service including computation on a server controlled by an operator, the method comprising:

moving a selected portion of said computation from a server controlled by said operator into a trusted co-server executing inside a secure coprocessor;

allowing clients to interact with the server through the co-server; and

using the trusted co-server as a trusted third party to authenticate interactions between the client and the server; and

wherein the moving step includes the steps of

i) installing a device private/public key pair on the co-server,

ii) installing co-server application software in the trusted co-server, said ~~co-sever~~ co-server application software having an ability to authenticate itself ~~using~~ with said device key pair,

iii) the co-server application software then generating an application key pair including a public key and a private key, [[;]]

iv) using the co-server application's ability to authenticate itself ~~and~~ with said device key pair to prove to a certificate authority that said application key pair belongs to an installation of said ~~co-sever~~ co-server application,

v) the certificate authority then issuing a certificate attesting to the public key of said application key pair and the entity to which said public key belongs, and

vi) the co-server application storing said certificate,

the step of using the trusted co-server includes the steps of

i) establishing a session between the client and the co-server application, and

ii) indicating to the client that the co-server application demonstrates knowledge of the private key of said application key pair to provide assurance of the authenticity of communication from the trusted co-server.

33. (Currently Amended) A method for enhancing a service including computation on a server controlled by an operator, the method comprising:

providing at least one security and privacy property to at least one client ~~from~~ of a plurality of clients by:

moving a selected portion of said computation from a server controlled by said operator into a trusted co-server executing inside a secure coprocessor;

enabling clients to interact with the server and the co-server; and

using the trusted co-server as a trusted third party to authenticate interactions between the client and the server; and

wherein the moving step includes the steps of

i) installing a device private/public key pair on the co-server,

ii) installing co-server application software in the trusted co-server, said ~~co-sever~~ co-server application software having an ability to authenticate itself using said device key pair,

iii) the co-server application software then generating an application key pair including a public key and a private key, [[;]]

iv) using the co-server application's ability to authenticate itself ~~and~~ with said device key pair to prove to a certificate authority that said application key pair belongs to an installation of said ~~co-sever~~ co-server application,

v) the certificate authority then issuing a certificate attesting to the public key of said application key pair and the entity to which said public key belongs, and

vi) the co-server application storing said certificate,

the step of using the trusted co-server includes the steps of

i) establishing a session between the client and the co-server application, and

ii) indicating to the client that the co-server application demonstrates knowledge of the private key of said application key pair to provide assurance of the authenticity of communication from the trusted co-server.

Claim 34. (Currently Amended) A trusted co-server, executing a program such that:

for multiple parties, including a Web server, a remote client and said co-server, each party provides input, and then the co-server carries out for each party, a function on all these inputs, and output to said each party; and

wherein the co-server executes so as to authenticate interactions between the client and the Web server so that said parties can authenticate and trust the correct execution of the co-server, in interactions between the client and the co-server, despite attempts by the Web server to subvert said execution; and

wherein a device private/public key pair and co-server application software is installed in the trusted co-server, said co-server application software having an ability to authenticate itself using said device key pair, and said co-server application software generates an application key pair including a public key and a private key, said co-server authenticates itself using said device key pair to prove to a certificate authority that said application key pair belongs to an installation of said co-server application, the certificate authority then issues a certificate attesting to the public key of said application key pair and the entity to which said public key pair ~~and the entity to which said public key~~ belongs, and the co-server application stores said certificate, and when a session is established between the client and the co-server application, the client is informed that the co-server application has knowledge of the private key of said key pair to provide assurance of the authenticity of communications from the trusted co-server.

Claim 37. (Currently Amended) A method of enhancing the security of a Web based transaction utilizing a server, the method comprising the steps:

providing the server with a trusted co-server; and

using the trusted co-server to execute a program such that:

for multiple parties,

each party provides input and then said co-server carries out for each party, a function on all these inputs to authenticate interactions between the party and the server and the parties trust interactions between the parties and the server, and

wherein a device private/public key pair and co-server application software is installed in the trusted co-server, said co-server application software having an ability to authenticate itself using said device key pair, and said co-server application software generates a key pair including a public key and a private key, said co-server authenticates itself using said device key pair to prove to a certificate authority that said application key pair belongs to an installation of said co-server application, the certificate authority then issues a certificate attesting to the public key of said application key pair and the entity to which said public key pair ~~and the entity to which said public key~~ belongs, and the co-server application stores said certificate, and when a session is established between the client and the co-server application, the client is informed that the co-server application has knowledge of the private key of said key pair to provide assurance of the authenticity of communications from the trusted co-server.

Claim 39. (Currently Amended) A method according to Claim 37, where:

the client authenticates the co-server, the client sends its input to the co-server over a private channel, and the co-server sends its output to said another party over a private channel~~, such as one established by encryption with a shared secret key~~.

Claim 40. (Currently Amended) A program storage device readable by machine, tangibly embodying a program of instructions executable by the machine to perform method steps for enhancing a computational service to at least one client of a plurality of clients, said method steps comprising:

moving a selected portion of a computation from a server into a trusted co-server executing inside a secure coprocessor;

allowing each client to interact with the server and the co-server; and

using the trusted co-server as a trusted third party to authenticate interactions between the client and the server; and

wherein the moving step includes the steps of:

i) installing a device private/public key pair on the co-server,

ii) installing co-server application software in the trusted co-server, said ~~co-sever~~ co-server application software having an ability to authenticate itself using said device key pair,

iii) the co-server application software then generating an application key pair including a public key and a private key, [[;]]

iv) using the co-server application's ability to authenticate itself ~~and~~ with said device key pair to prove to a certificate authority that said application key pair belongs to an installation of said ~~co-sever~~ co-server application,

v) the certificate authority then issuing a certificate attesting to the public key of said application key pair and the entity to which said public key belongs, and

vi) the co-server application storing said certificate,

the step of using the trusted co-server includes the steps of

i) establishing a session between the client and the co-server application, and

ii) indicating to the client that the co-server application demonstrates knowledge of the private key of said application key pair to provide assurance of the authenticity of communication from the trusted co-server.

Claim 42. (Currently Amended) A program storage device according to Claim 41, wherein the step of allowing includes enabling said each client an authenticated, private channel to said co-server.

Claim 43. (Currently Amended) A method according to Claim 1, wherein:

the moving step includes the step of an operator of the server using a secure coprocessor platform to install and certify the trusted co-server, including the steps of

i) the server operator obtaining a secure coprocessor platform,

ii) the server operator installing the co-server application software into the secure coprocessor platform,

the establishing step includes the steps of

i) establishing an SSL session between the client and the trusted co-server, and

ii) the client using a Web browser to initiate an SSL session with the co-server application within the secure co-processor at a Web site maintained by the server operator, [[;]] and

the indicating step includes the step of said Web browser indicating to the client that the co-server application demonstrates knowledge of the private key of said generated application key pair.

Claim 44. (Currently Amended) A method according to Claim 43, wherein the using step includes the further steps of:

the client opening an SSL session to the trusted co-server, said trusted co-server being configured with a payment application, including the steps of

i) the server forwarding a price to the co-server,

ii) the co-server then displaying said price and accepting private credit card information of the client,

iii) the co-server signing and encrypting said price and said private credit card information, and

iv) the server operator then injecting said encrypted price and credit card information into a payment system;

the client opening an SSL session with a trusted co-server configured with a server status application, including the step of the co-server displaying authenticated information to the client about the server and providing a link by which the client can connect to the server; and

the client opening an SSL session with the trusted co-server, said trusted co-server being configured with an authentication application, including the steps of

i) the co-server prompting the client for client authentication information, including a ~~used~~ user id and password,

ii) the client providing said authentication information,

iii) the co-server verifying the authenticity of said information, then directing the client to the server, and providing the server with an authentication token indicating that the client has properly authenticated.

Response to Arguments

2. The Non-Final response filed on 7/28/2006 has been entered. In response to the communications filed on 7/28/2006, Applicant has incorporated some of the limitations of claim 43 into the independent claims and further amended the claims to better define the subject matter of these claims. Applicant's arguments filed on 7/28/2006 have been fully considered and they are persuasive as amended. In an interview held with the Examiner on November 6, 2006, the Examiner suggested Applicant's attorney, John Sensny to correct the informalities in the claims and better clarify some of the claim limitations as shown above in the Examiner's amendment.

Reasons for Allowance

3. The following is an examiner's statement of reasons for allowance: the prior art of record US Patent 6,453,296 to Iwamura discloses client/server authentication in an electronic credit system using key pair and trusted party. The Non-Patent Literature by Wilhelml, U., et al

discloses installing trusted application in a co-server and verifying that the agents and the co-server are trusted entities, the agent in one embodiment uses a certificate authority to guarantee the public key of the trusted party. US Patent 6,643,701 to Aziz et al discloses client-server environment using SSL secure communication wherein a client using a Web browser to initiate an SSL session with a trusted co-server application in a Web site environment and further discloses the co-server application software generates a key pair including a public key and a private key; and when an SSL session is established between the client and the co-server application, the client is informed that the co-server application has knowledge of the private key of said key pair. The prior arts of record, however, fail to teach singly or in combination: installing co-server application software in the trusted co-server, said co-server application software having an ability to authenticate itself using said device key pair, the co-server application software then generating an application key pair including a public key and a private key; using the co-server application's ability to authenticate itself with said device key pair to prove to a certificate authority that said application key pair belongs to an installation of said co-server application indicating to the client that the co-server application demonstrates knowledge of the private key of said application key pair to provide assurance of the authenticity of communication from the trusted co-server as claimed in the independent claims 1, 31, 33, 34, 37, and 40. Consequently, independent claims 1, 31, 33, 34, 37, and 40 are allowable over the prior arts of record. Claims 2-22, 25-30, 32, 35-36, 38-39, and 41-44 are directly or indirectly dependent upon claims 1, 31, 33, 34, 37, and 40, and therefore are also allowable over the prior arts of record.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

4. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Carl Colin whose telephone number is 571-272-3862. The examiner can normally be reached on Monday through Thursday, 8:00-6:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser G. Moazzami can be reached on 571-272-4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

cc

Carl Colin
Patent Examiner
November 9, 2006

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

11/09/06